

2012 IEEE 53rd Annual Symposium on Foundations of Computer Science

(FOCS 2012)

**New Brunswick, New Jersey, USA
20-23 October 2012**



**IEEE Catalog Number: CFP12053-PRT
ISBN: 978-1-4673-4383-1**

2012 IEEE 53rd Annual Symposium on Foundations of Computer Science

FOCS 2012

Table of Contents

| | |
|---------------------------|-----|
| Foreword..... | xii |
| Organizing Committee..... | xiv |
| Program Committee..... | xv |
| Reviewers..... | xvi |
| Awards..... | xix |

Session 1A

| | |
|--|----|
| Learning Topic Models—Going beyond SVD | 1 |
| <i>Sanjeev Arora, Rong Ge, and Ankur Moitra</i> | |
| Finding Correlations in Subquadratic Time, with Applications to Learning Parities and Juntas | 11 |
| <i>Gregory Valiant</i> | |
| Active Property Testing..... | 21 |
| <i>Maria-Florina Balcan, Eric Blais, Avrim Blum, and Liu Yang</i> | |

Session 1B

| | |
|---|----|
| How to Compute in the Presence of Leakage | 31 |
| <i>Shafi Goldwasser and Guy N. Rothblum</i> | |
| Positive Results for Concurrently Secure Computation in the Plain Model | 41 |
| <i>Vipul Goyal</i> | |
| Constructing Non-malleable Commitments: A Black-Box Approach | 51 |
| <i>Vipul Goyal, Chen-Kuei Lee, Rafail Ostrovsky, and Ivan Visconti</i> | |

Session 2A

| | |
|---|----|
| Constructive Discrepancy Minimization by Walking on the Edges | 61 |
| <i>Shachar Lovett and Raghu Meka</i> | |
| Combinatorial Coloring of 3-Colorable Graphs | 68 |
| <i>Ken-ichi Kawarabayashi and Mikkel Thorup</i> | |
| A Permanent Approach to the Traveling Salesman Problem | 76 |
| <i>Nisheeth K. Vishnoi</i> | |

| | |
|---|----|
| Split and Join: Strong Partitions and Universal Steiner Trees for Graphs | 81 |
| <i>Costas Busch, Chinmoy Dutta, Jaikumar Radhakrishnan, Rajmohan Rajaraman, and Srivathsan Srinivasagopalan</i> | |

Session 2B

| | |
|---|-----|
| A Structure Theorem for Poorly Anticoncentrated Gaussian Chaoses and Applications to the Study of Polynomial Threshold Functions | 91 |
| <i>Daniel M. Kane</i> | |
| Large Deviation Bounds for Decision Trees and Sampling Lower Bounds for AC0-Circuits | 101 |
| <i>Chris Beck, Russell Impagliazzo, and Shachar Lovett</i> | |
| Pseudorandomness from Shrinkage | 111 |
| <i>Russell Impagliazzo, Raghu Meka, and David Zuckerman</i> | |
| Better Pseudorandom Generators from Milder Pseudorandom Restrictions | 120 |
| <i>Parikshit Gopalan, Raghu Meka, Omer Reingold, Luca Trevisan, and Salil Vadhan</i> | |

Session 3A

| | |
|--|-----|
| Optimal Multi-dimensional Mechanism Design: Reducing Revenue to Welfare Maximization | 130 |
| <i>Yang Cai, Constantinos Daskalakis, and S. Matthew Weinberg</i> | |
| The Exponential Mechanism for Social Welfare: Private, Truthful, and Nearly Optimal | 140 |
| <i>Zhiyi Huang and Sampath Kannan</i> | |
| Concave Generalized Flows with Applications to Market Equilibria | 150 |
| <i>László A. Végh</i> | |

Session 3B

| | |
|--|-----|
| Efficient Interactive Coding against Adversarial Noise | 160 |
| <i>Zvika Brakerski and Yael Tauman Kalai</i> | |
| A Direct Product Theorem for the Two-Party Bounded-Round Public-Coin Communication Complexity | 167 |
| <i>Rahul Jain, Attila Pereszlényi, and Penghui Yao</i> | |
| An Additive Combinatorics Approach Relating Rank to Communication Complexity | 177 |
| <i>Eli Ben-Sasson, Shachar Lovett, and Noga Ron-Zewi</i> | |

Session 4A

| | |
|---|-----|
| Approximating the Expansion Profile and Almost Optimal Local Graph Clustering | 187 |
| <i>Shayan Oveis Gharan and Luca Trevisan</i> | |
| Faster SDP Hierarchy Solvers for Local Rounding Algorithms | 197 |
| <i>Venkatesan Guruswami and Ali Kemal Sinop</i> | |

Session 4B

| | |
|---|-----|
| Learning-Graph-Based Quantum Algorithm for k-Distinctness | 207 |
| <i>Aleksandrs Belovs</i> | |
| A PTAS for Computing the Supremum of Gaussian Processes | 217 |
| <i>Raghu Meka</i> | |

Session 5

| | |
|---|-----|
| From the Impossibility of Obfuscation to a New Non-Black-Box Simulation Technique | 223 |
| <i>Nir Bitansky and Omer Paneth</i> | |
| A Polylogarithmic Approximation Algorithm for Edge-Disjoint Paths with Congestion 2 | 233 |
| <i>Julia Chuzhoy and Shi Li</i> | |
| A Multi-prover Interactive Proof for NEXP Sound against Entangled Provers | 243 |
| <i>Tsuyoshi Ito and Thomas Vidick</i> | |

Session 6A

| | |
|--|-----|
| Beck's Three Permutations Conjecture: A Counterexample and Some Consequences | 253 |
| <i>Alantha Newman, Ofer Neiman, and Aleksandar Nikolov</i> | |
| Iterative Rounding Approximation Algorithms for Degree-Bounded Node-Connectivity Network Design | 263 |
| <i>Takuro Fukunaga and R. Ravi</i> | |
| LP Rounding for k-Centers with Non-uniform Hard Capacities | 273 |
| <i>Marek Cygan, MohammadTaghi Hajiaghayi, and Samir Khuller</i> | |

Session 6B

| | |
|---|-----|
| On-Line Indexing for General Alphabets via Predecessor Queries on Subsets of an Ordered List | 283 |
| <i>Tsvi Kopelowitz</i> | |
| Higher Cell Probe Lower Bounds for Evaluating Polynomials | 293 |
| <i>Kasper Green Larsen</i> | |
| The Tile Assembly Model is Intrinsically Universal | 302 |
| <i>David Doty, Jack H. Lutz, Matthew J. Patitz, Robert T. Schweller, Scott M. Summers, and Damien Woods</i> | |

Session 7A

| | |
|---|-----|
| The Dynamics of Influence Systems | 311 |
| <i>Bernard Chazelle</i> | |
| The Locality of Distributed Symmetry Breaking | 321 |
| <i>Leonid Barenboim, Michael Elkin, Seth Pettie, and Johannes Schneider</i> | |
| How to Allocate Tasks Asynchronously | 331 |
| <i>Dan Alistarh, Michael A. Bender, Seth Gilbert, and Rachid Guerraoui</i> | |

| | |
|--|-----|
| Tight Bounds for Randomized Load Balancing on Arbitrary Network Topologies | 341 |
| <i>Thomas Sauerwald and He Sun</i> | |

Session 7B

| | |
|---|-----|
| On the Complexity of Finding Narrow Proofs | 351 |
| <i>Christoph Berkholz</i> | |
| The Computational Hardness of Counting in Two-Spin Models on d-Regular Graphs | 361 |
| <i>Allan Sly and Nike Sun</i> | |
| Making the Long Code Shorter | 370 |
| <i>Boaz Barak, Parikshit Gopalan, Johan Håstad, Raghu Meka, Prasad Raghavendra, and David Steurer</i> | |
| Hardness of Finding Independent Sets in Almost q-Colorable Graphs | 380 |
| <i>Subhash Khot and Rishi Saket</i> | |

Session 8A

| | |
|---|-----|
| Population Recovery and Partial Identification | 390 |
| <i>Avi Wigderson and Amir Yehudayoff</i> | |
| The Privacy of the Analyst and the Power of the State | 400 |
| <i>Cynthia Dwork, Moni Naor, and Salil Vadhan</i> | |
| The Johnson-Lindenstrauss Transform Itself Preserves Differential Privacy | 410 |
| <i>Jeremiah Blocki, Avrim Blum, Anupam Datta, and Or Sheffet</i> | |

Session 8B

| | |
|---|-----|
| On Range Searching with Semialgebraic Sets II | 420 |
| <i>Pankaj K. Agarwal, Jiří Matoušek, and Micha Sharir</i> | |
| Down the Rabbit Hole: Robust Proximity Search and Density Estimation in Sublinear Space | 430 |
| <i>Sariel Har-Peled and Nirman Kumar</i> | |
| On the Homotopy Test on Surfaces | 440 |
| <i>Francis Lazarus and Julien Rivaud</i> | |

Session 9A

| | |
|--|-----|
| Representative Sets and Irrelevant Vertices: New Tools for Kernelization | 450 |
| <i>Stefan Kratsch and Magnus Wahlström</i> | |
| Designing FPT Algorithms for Cut Problems Using Randomized Contractions | 460 |
| <i>Rajesh Chitnis, Marek Cygan, MohammadTaghi Hajiaghayi, Marcin Pilipczuk, and Michał Pilipczuk</i> | |
| Planar F-Deletion: Approximation, Kernelization and Optimal FPT Algorithms | 470 |
| <i>Fedor V. Fomin, Daniel Lokshantov, Neeldhara Misra, and Saket Saurabh</i> | |

Session 9B

| | |
|--|-----|
| Approximation Limits of Linear Programs (Beyond Hierarchies) | 480 |
| <i>Gábor Braun, Samuel Fiorini, Sebastian Pokutta, and David Steurer</i> | |
| Formulas Resilient to Short-Circuit Errors | 490 |
| <i>Yael Tauman Kalai, Allison Lewko, and Anup Rao</i> | |
| Lower Bounds on Information Complexity via Zero-Communication Protocols and Applications | 500 |
| <i>Jordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao</i> | |

Session 10—Knuth Prize Lecture

| | |
|-------------------------------|-----|
| Rarity for Semimeasures | 510 |
| <i>Leonid A. Levin</i> | |

Session 11A

| | |
|---|-----|
| Faster Algorithms for Rectangular Matrix Multiplication | 514 |
| <i>François Le Gall</i> | |
| Quasi-optimal Multiplication of Linear Differential Operators | 524 |
| <i>Alexandre Benoit, Alin Bostan, and Joris van der Hoeven</i> | |
| Algorithmic Applications of Baur-Strassen’s Theorem: Shortest Cycles, Diameter and Matchings | 531 |
| <i>Marek Cygan, Harold N. Gabow, and Piotr Sankowski</i> | |

Session 11B

| | |
|--|-----|
| Almost Optimal Canonical Property Testers for Satisfiability | 541 |
| <i>Christian Sohler</i> | |
| Partially Symmetric Functions Are Efficiently Isomorphism-Testable | 551 |
| <i>Eric Blais, Amit Weinstein, and Yuichi Yoshida</i> | |
| Sparse Affine-Invariant Linear Codes Are Locally Testable | 561 |
| <i>Eli Ben-Sasson, Noga Ron-Zewi, and Madhu Sudan</i> | |

Session 12A

| | |
|---|-----|
| The Cutting Plane Method Is Polynomial for Perfect Matchings | 571 |
| <i>Karthekeyan Chandrasekaran, László A. Végh, and Santosh Vempala</i> | |
| A Weight-Scaling Algorithm for Min-Cost Imperfect Matchings in Bipartite Graphs | 581 |
| <i>Lyle Ramshaw and Robert E. Tarjan</i> | |
| A New Direction for Counting Perfect Matchings | 591 |
| <i>Taisuke Izumi and Tadashi Wadayama</i> | |
| Single Source—All Sinks Max Flows in Planar Digraphs | 599 |
| <i>Jakub Łącki, Yahav Nussbaum, Piotr Sankowski, and Christian Wulff-Nilsen</i> | |

Session 12B

| | |
|--|-----|
| New Limits to Classical and Quantum Instance Compression | 609 |
| <i>Andrew Drucker</i> | |
| Lower Bounds on Interactive Compressibility by Constant-Depth Circuits | 619 |
| <i>Arkadev Chattopadhyay and Rahul Santhanam</i> | |
| Geometric Complexity Theory V: Equivalence between Blackbox Derandomization of Polynomial Identity Testing and Derandomization of Noether’s Normalization Lemma | 629 |
| <i>Ketan D. Mulmuley</i> | |
| Computing Multiplicities of Lie Group Representations | 639 |
| <i>Matthias Christandl, Brent Doran, and Michael Walter</i> | |

Session 13A

| | |
|--|-----|
| A Tight Linear Time (1/2)-Approximation for Unconstrained Submodular Maximization | 649 |
| <i>Niv Buchbinder, Moran Feldman, Joseph (Seffi) Naor, and Roy Schwartz</i> | |
| A Tight Combinatorial Algorithm for Submodular Maximization Subject to a Matroid Constraint | 659 |
| <i>Yuval Filmus and Justin Ward</i> | |
| The Power of Linear Programming for Valued CSPs | 669 |
| <i>Johan Thapper and Stanislav Živný</i> | |

Session 13B

| | |
|---|-----|
| How to Construct Quantum Random Functions | 679 |
| <i>Mark Zhandry</i> | |
| Non-malleable Extractors, Two-Source Extractors and Privacy Amplification | 688 |
| <i>Xin Li</i> | |
| Constructing a Pseudorandom Generator Requires an Almost Linear Number of Calls | 698 |
| <i>Thomas Holenstein and Makrand Sinha</i> | |

Session 14A

| | |
|---|-----|
| Randomized Greedy Algorithms for the Maximum Matching Problem with New Analysis | 708 |
| <i>Matthias Poloczek and Mario Szegedy</i> | |
| Matching with Our Eyes Closed | 718 |
| <i>Gagan Goel and Pushkar Tripathi</i> | |
| Online Matching with Stochastic Rewards | 728 |
| <i>Aranyak Mehta and Debmalya Panigrahi</i> | |

Session 14B

| | |
|--|-----|
| A New Infinity of Distance Oracles for Sparse Graphs | 738 |
| <i>Mihai Pătraşcu, Liam Roditty, and Mikkel Thorup</i> | |

| | |
|--|-----|
| Improved Distance Sensitivity Oracles via Fast Single-Source Replacement Paths | 748 |
| <i>Fabrizio Grandoni and Virginia Vassilevska Williams</i> | |
| Everywhere-Sparse Spanners via Dense Subgraphs | 758 |
| <i>Eden Chlamtác, Michael Dinitz, and Robert Krauthgamer</i> | |
| Author Index | 768 |